DOCUMENT PUBLIC — VERSION 1.0 — 5 MAI 2026

Politique de sécurité de l'information

Document fondateur du système de management de la sécurité de l'information (SMSI) de Garante

La présente politique exprime l'engagement de la direction en matière de protection des données traitées dans le cadre du SaaS Garante et fixe le cadre des mesures techniques et organisationnelles appliquées. Garante n'est aujourd'hui pas certifié ISO/IEC 27001:2022. La politique s'appuie néanmoins sur les contrôles de l'Annexe A de cette norme et sur les obligations imposées par le RGPD, dans une logique de conformité progressive et d'amélioration continue.

1. Identification

Éditeur	Ahmed Bellafkih, exerçant sous le nom commercial Garante
Statut	Entreprise individuelle (micro-entrepreneur)
SIREN	988 920 617
Siège social	50 avenue des Champs-Élysées, 75008 Paris
Contact sécurité	security@garante.fr
Contact DPO interne	dpo@garante.fr
Périmètre du SMSI	Plateforme SaaS Garante (frontend, backend, infrastructure, sous-traitants ultérieurs)

2. Engagement de la direction

La direction de Garante s'engage à :

— Garantir la confidentialité, l'intégrité, la disponibilité et l'opposabilité des données traitées (Art. 32 RGPD).

— Allouer les ressources nécessaires au SMSI dans la mesure compatible avec la phase early-stage, avec transparence totale sur les arbitrages.

— Respecter les engagements contractuels pris envers les cabinets clients (Contrat de prestation, CGUV, DPA, liste des sous-traitants).

— Améliorer en continu le niveau de sécurité (revues régulières, retours d'expérience, évolutions réglementaires).

— Communiquer de manière honnête et publique sur les choix de sécurité, y compris sur les éléments non encore implémentés et leur calendrier d'engagement.

3. Référentiel et périmètre

Référentiel suivi

— Règlement (UE) 2016/679 (RGPD)

— Recommandations de la CNIL

— Contrôles de l'Annexe A de la norme ISO/IEC 27001:2022 (sans certification à ce jour)

— Recommandations de l'ANSSI applicables aux services numériques

Périmètre couvert

— L'application web Garante (frontend Next.js + backend Fastify)

— L'infrastructure d'hébergement (serveur Hetzner Falkenstein)

— Les sous-traitants ultérieurs déclarés sur la page publique /legal/subprocessors

— Les processus opérationnels associés (développement, déploiement, support, gestion des incidents)

Hors périmètre

— Les systèmes d'information internes des cabinets clients

— Les sous-traitants des cabinets clients (gérés directement dans leur propre registre)

— Les terminaux et postes de travail des utilisateurs finaux

4. Responsabilités

Responsable sécurité de l'information

Ahmed Bellafkih cumule, au stade actuel de l'entreprise, les fonctions de dirigeant, de RSSI et de DPO interne de Garante. Ce cumul transparent est documenté publiquement. Une séparation des fonctions sera engagée à l'embauche du premier collaborateur permanent.

Sous-traitants ultérieurs

Chaque sous-traitant ultérieur est lié contractuellement par les mêmes obligations que celles imposées à Garante par le DPA principal (Art. 28(4) RGPD). La liste exhaustive est publiée sur /legal/subprocessors.

Utilisateurs

Les utilisateurs sont tenus de respecter les bonnes pratiques de sécurité décrites dans les CGUV (mots de passe robustes, activation du 2FA, signalement immédiat de tout accès suspect).

5. Engagements opérationnels de sécurité

Confidentialité

— Multi-tenancy strict avec Row-Level Security PostgreSQL en production (rôle garante_app non superuser, NOBYPASSRLS)
— Chiffrement AES-256-GCM au repos pour tous les secrets sensibles en base
— MinIO SSE-KMS pour les fichiers stockés (DSAR, pièces d'identité, documents)
— TLS 1.3 in-transit sur tous les flux externes et internes
— 2FA TOTP obligatoire par défaut pour tous les rôles (administrateur, DPO, assistant)

Intégrité

— Audit trail tamper-evident par chaîne de hash SHA-256 sur DSAR, violations, AIPD et registres (opposabilité Art. 5.2 RGPD + Art. 1366 C. civ.)
— Validation Zod systématique de chaque entrée des API
— Code source versionné Git avec historique complet

Disponibilité

— Sauvegardes quotidiennes chiffrées AES-256-CBC avec dérivation PBKDF2 (100 000 itérations), rétention 30 jours glissants
— Copie hors-ligne rotative quotidienne sur stockage isolé du runtime applicatif (rétention 7 jours)
— Réplication off-site géographique (souveraineté UE) engagée à compter de la signature du premier client payant
— Procédure de restauration documentée et testée à chaque déploiement majeur incluant migration de schéma
— Service fourni en mode best effort, sans engagement de SLA chiffré (cf. CGUV Art. 13)

Opposabilité

— Audit trail SHA-256 chaîné couvrant DSAR, violations, AIPD et registres (Art. 5.2 RGPD + Art. 1366 C. civ.)
— Bundle d'export incluant manifest SHA-256 par fichier et signature globale
— Conservation des logs d'audit dans les durées définies par le DPA et la procédure de notification de violation

6. Engagements quantifiés

Délai de réponse à un signalement de faille (security.txt)	48 heures
Test de restauration des sauvegardes	À chaque déploiement majeur (incluant migration Prisma)
Audit interne de sécurité	Annuel
Mise à jour du registre des risques	Annuelle + sur événement majeur
Évaluation des sous-traitants ultérieurs (vendor assessment)	Annuelle

Revue de la présente politique	Annuelle
Délai de rédaction d'un post-mortem après incident	30 jours
Notification d'un incident impactant le service au client	48 heures ouvrées
Programme de récompense de signalement (bug bounty)	Aucune récompense financière — remerciement public sur demande
Formation sécurité (dirigeant et futurs collaborateurs)	Annuelle, auto-formation documentée
Notification d'une violation de données au client (DPA Art. 4.7.1)	48 heures suivant détection

7. Gestion des incidents et continuité

Procédure formalisée en quatre étapes : (1) détection et qualification ; (2) confinement et remédiation immédiate ; (3) notification des parties concernées dans les délais réglementaires (48 heures pour les clients, 72 heures pour la CNIL) ; (4) post-mortem écrit dans les 30 jours.

En cas d'indisponibilité totale du Service supérieure à 72 heures consécutives imputable à Garante, le client peut résilier sans préavis et obtenir le remboursement prorata temporis du mois en cours (CGUV Art. 13.2).

8. Revue et amélioration continue

La présente politique fait l'objet d'une revue annuelle par la direction. Une revue exceptionnelle est déclenchée en cas d'événement majeur (incident significatif, nouveau sous-traitant ultérieur, évolution réglementaire substantielle, embauche du premier collaborateur permanent).

Indicateurs suivis : nombre d'incidents de sécurité par criticité, signalements de faille reçus et délai moyen de réponse, résultats des tests de restauration (succès / échec, RTO observé), conformité des sous-traitants ultérieurs, vulnérabilités identifiées dans les dépendances logicielles.

9. Documents associés

— Architecture de sécurité technique détaillée — /legal/securite
— Analyse d'impact relative à la protection des données du SaaS Garante — /legal/aipd
— Liste des sous-traitants ultérieurs — /legal/subprocessors
— DPA et mesures techniques et organisationnelles (TOMs) — /legal/dpa
— Politique de confidentialité — /legal/privacy
— Conditions générales d'utilisation et de vente — /legal/terms
— Contrat de prestation SaaS — sur demande à contact@garante.fr

10. Approbation

Politique approuvée et signée par :

Ahmed Bellafkih
Dirigeant et Responsable de la sécurité de l'information
Garante — SIREN 988 920 617

Fait à Paris, le 5 mai 2026

Version 1.0 — 5 mai 2026 — Prochaine revue prévue : mai 2027 (ou avant en cas d'événement majeur)